



## **La metamorfosis “inteligente” de las fronteras y su alcance ambivalente en el control migratorio europeo. Un punto de no retorno**

**(The ‘smart’ metamorphosis of borders and their ambivalent scope in the European migration control. A line in the sand)**

OÑATI SOCIO-LEGAL SERIES FORTHCOMING

DOI LINK: <https://doi.org/10.35295/OSLS.IISL.2418>

RECEIVED 3 JULY 2025, ACCEPTED 22 DECEMBER 2025, FIRST-ONLINE PUBLISHED 21 JANUARY 2026

ENCARNACIÓN LA SPINA\* 

### **Resumen**

El proceso de transformación digital de las fronteras exteriores europeas y, especialmente la capacidad de inferencia de las fronteras inteligentes ha cambiado y seguirá cambiando la forma de anticipar, controlar y frenar los flujos migratorios hacia la Unión Europea. No solo a través del uso generalizado de herramientas predictivas, sistemas de identificación biométrica remota y sistemas de verificación cruzada, sino también por medio de la puesta en práctica de diferentes sistemas de tecnología inteligente. Actualmente, una multitud de nuevas aplicaciones tecnológicas y la creciente interoperabilidad de los sistemas TI a gran escala está tratando de dar una respuesta eficiente, objetiva y sostenible a la gestión fronteriza de la inmigración y del asilo. Esta transformación “inteligente” de los confines fronterizos aparentemente inocua contribuye, desde un enfoque centrado en la seguridad y menos crítico, a la reproducción ilimitada de categorías estereotipadas sobre las movilidades (no) deseadas o sospechosas.

### **Palabras clave**

Fronteras inteligentes; sistemas TI a gran escala; migrantes; categorías estereotipadas; Unión Europea

---

Este trabajo se ha realizado con el apoyo del Proyecto Derechos Humanos y Retos Socioculturales en un Mundo en Transformación (ref.: IT1468-22) y del Proyecto I+D+i RESEST «Resiliencia del derecho antidiscriminatorio a los sesgos y estereotipos: desafíos y propuestas de intervención» (ref. PID2021-123171OB-I00), del Ministerio de Ciencia e Innovación.

\* Encarnación La Spina. Universidad de Deusto. Email: [elaspina@deusto.es](mailto:elaspina@deusto.es) ORCID: <https://orcid.org/0000-0003-0423-0674>

## Abstract

The process of digital transformation of Europe's external borders, and especially the inference capacity of smart borders, has changed and will continue to change the way migration flows into the European Union are anticipated, controlled, and managed. Not only through the widespread use of predictive tools, remote biometric identification, and cross-verification systems, but also through the implementation of various AI-based technological systems. Currently, a myriad of new high-tech applications and the interoperability of large IT systems are attempting to provide an efficient, objective, and sustainable response to border management in relation to immigration and asylum. This seemingly innocuous 'intelligent' transformation of borders contributes, from a security-focused and less critical perspective, to the unlimited reproduction of stereotyped categories regarding (un)desired or suspicious mobilities.

## Key words

Smart borders; IT systems; migrants; stereotyped categories; European Union

## Table of contents

1. Introduction .....	4
2. La transformación inteligente de la frontera: génesis y alcance conceptual .....	6
3. Las <i>smart borders</i> como complejo ecosistema digital: una retrospectiva sobre el proceso de tecnificación de la frontera .....	8
3.1. Desde la creación de sistemas TI a gran escala hasta su interoperabilidad .....	8
3.2. Las líneas de transformación futuras de las Smart borders: el Nuevo Pacto europeo de migración y asilo y el Reglamento IA .....	13
4. Hacia la reproducción ilimitada e invisible de categorías migrantes estereotipadas a través de las <i>smart borders</i> .....	17
5. Reflexiones finales .....	22
Referencias .....	23

## 1. Introduction

En el siglo XXI, la Unión Europea (UE) y los Estados Unidos (EE. UU.) han dado un gran impulso a los procesos de digitalización y tecnificación de sus fronteras (Everuss 2021, 339, EMN-European Migration Network 2022, 11, Ozkul 2023, 64 y 40); al igual que lo han hecho otros países como Canadá, Australia y China (Molnar 2024). Este despliegue avanzado y generalizado de los procesos tecnológicos de la biometría, la vigilancia de datos (Van Dijck 2014) y la automatización en tándem (Pötzsch 2015, Forti 2024) implica una metamorfosis sin precedentes de la arquitectura fronteriza. Ello es así, no solo por la posibilidad de comprobaciones de identidad, verificación cruzada de datos, detección y prevención de flujos migratorios no deseados o sospechosos sino por involucrar al mismo tiempo en el proceso diferentes actores gubernamentales, el sector tecnológico privado (Csernatoní 2018, 177, Molnar 2019, 306) así como las diferentes agencias europeas u organizaciones internacionales (Marin 2011, 145, Leese 2014, 495).

Sobre la morfología cambiante de la frontera existen diferentes estudios interdisciplinarios que brindan una detallada evolución de este “espacio geográfico protegido y vigilado por el control del Estado”, especialmente aquellos relacionados con el ámbito de las migraciones y la seguridad (Campesi 2021, Velasco 2025). No en vano, las fronteras ya sea en sus confines territoriales tradicionales o en su contemporánea reconfiguración como “fronteras inteligentes” (*smart borders*) han tenido siempre y tienen una conexión intrínseca con los procesos y las prácticas de securitización, externalización y criminalización dirigidas hacia el fenómeno migratorio. Un fenómeno social complejo considerado *prima facie* como un peligro o riesgo para el orden público, una amenaza político-identitaria y una amenaza socio-económica (Campesi 2012, 6-8, Bigo 2022).

Precisamente, con el propósito de comprender mejor su entidad y alcance, desde los principales enfoques críticos, los estudios clásicos sobre seguridad y frontera han analizado principalmente la interacción de los diferentes actores involucrados en la frontera en el marco de la “gobernanza de la seguridad” (Leese 2016, 413), mientras que los “critical border studies” han puesto mayormente el foco en cómo se desarrollan o justifican las diferentes prácticas contemporáneas de *bordering* y *re-bordering*. Así lo han hecho para recalcar la compleja naturaleza de este “confín biopolítico generalizado”, conscientes de su amplia capacidad de producción de subjetividad en la gestión de la movilidad y en el gobierno de los cuerpos móviles (Vaughan-Williams 2009, 746). Todo ello, sin perjuicio de las aportaciones epistémicas de los “critical data studies” respecto a la capacidad generativa de “ansiedades o imaginarios asociados a bases de datos de gran magnitud” (Bellanova y Glouftsiou 2022, 460). En particular, respecto a la transición contemporánea de las fronteras globales, son varios los expertos que han destacado los efectos perversos de la deslocalización y la desterritorialización del control migratorio fronterizo (Balibar 2005, 89) bajo la máxima de que “los confines ya no están en el confín” sino que son fronteras movedizas o difusas (Côté-Boucher 2008), caracterizadas por su portabilidad, por la ductilidad de los datos allí recogidos (Taylor y Meissner 2020) y, por su interoperabilidad. Por tanto, a partir de la implementación progresiva de las “fronteras inteligentes” (Broeders 2007) es posible constatar cómo se ha instaurado un régimen de desagregación de confines múltiples (Sassen 2006, 524-525) y cómo a través

de este se ha ido dando paso a una constelación de puntos conectados de intercambio de informaciones o de recogida de datos orientados a la futura gestión integral de riesgos.

En paralelo, junto a estos enfoques teóricos reveladores de un cambio de paradigma sobre la nueva naturaleza de las fronteras, también en las últimas décadas se han ido sucediendo una gran variedad de análisis que ponen el foco en las particularidades y ambivalencias asociadas a las *smart borders* como nuevas formas de control y gestión migratoria (Everuss 2021, 355, Beduschi y McAuliffe 2022, Ozkul 2023, Goldner Lang 2024, Korkmaz 2024). Desde principios de la década de 2000, los estudios interdisciplinares sobre los regímenes fronterizos han señalado la creciente importancia de las infraestructuras digitales, el uso de la biometría para la gobernanza de la movilidad transfronteriza (Broeders 2007, Dijstelbloem y Meijer 2011) así como desde los “critical data studies” se ha insistido en los efectos de la recogida masiva o granular de datos. Tanto en los estudios sobre las fronteras como sobre las migraciones, las investigaciones críticas han hecho especial hincapié en las nuevas tecnologías empleadas en el control fronterizo, cuestionando así las posiciones de los actores y las racionalidades subyacentes al *tecnosolucionismo*. Esto es, tanto sus discursos de inclusión/exclusión como la necesidad de políticas de mayor securitización y fortalecimiento del control fronterizo (Burgess y Kloza 2021, 25). Entre los desafíos señalados en tales estudios abunda y destaca especialmente la prioridad dada a la protección de datos sin perjuicio de las implicaciones ético-jurídicas y las advertencias sobre los derechos humanos en riesgo para aquellos colectivos vulnerables o en situación de vulnerabilidad (Avello Martínez 2023, Garrido Carrillo 2023). Sin embargo, a pesar de las diferentes voces críticas sobre la seguridad, objetividad, eficiencia y sostenibilidad económica, resulta paradójico que los impactos discriminatorios directos e indirectos se encuentren menos definidos y abordados en los debates actuales. Por ejemplo, así ocurre ante los efectos imprevisibles de la llamada “function creep” o “surveillance creep” sobre las personas migrantes que como “población cautiva” se vuelven más y más cognoscibles, calculables y gobernables.

No en vano, entre los sectores poblaciones, las personas nacionales de terceros países son y van a ser con creces aquellas más expuestas al cruce fronterizo inteligente y también han sido objeto históricamente de discriminaciones directas e indirectas (Broeders 2007, 2011, Trauttmansdorff 2017, Achiume 2022). De ahí que la creciente selectividad y (semi)permeabilidad de estas fronteras (Walters 2006, 197) así como la irrupción de la biometría o de herramientas IA de gestión de la identidad basada en el riesgo (Muller 2009) acentuarán si cabe más la gestión diferencial o la verificación cruzada integral de las circulaciones negativas y positivas (Agamben 2006) por medio de sistemas que operan como filtros (*firewall*) para “distinguir lo bueno de lo malo, lo útil de lo peligroso, lo lícito de lo ilícito” (Nobile 2024, 300-301). En su conjunto el funcionamiento deseado de estas fronteras, permite diferenciar entre la movilidad económicamente favorable o el *modus operandi* de la buena circulación y de aquella peligrosa legítimamente excluida mediante fronteras que estratifican los derechos y los riesgos (Foucault 2008, 18 y 42). Por ello, ciertos autores persisten en recordar las implicaciones biopolíticas de estas fronteras dados los múltiples significados que conlleva el uso de dispositivos biométricos (Amoore 2006, 338) o el *re-bordering* (Leese 2016, 415, Leese *et al.* 2022), así como su portabilidad *elsewhere* (Lyon 2005). No en vano, son formas descentralizadas y externalizadas de control estatal sobre los cuerpos que,

desde diferentes finalidades e intensidades, implican una nueva era en el gobierno global de la movilidad y en la elaboración de perfiles de comportamientos sospechosos o indeseados (Everuss 2021, 339), especialmente por sus ramificaciones en la lucha contra el terrorismo, la delincuencia o la migración irregular.

Por todo ello, sin duda, un buen laboratorio de análisis sobre el trasfondo crítico de esta transformación inteligente de la frontera es su compleja configuración técnico-normativa desde los diferentes *smart borders packages* hasta la plena operatividad del marco de interoperabilidad. Una configuración y arquitectura fronteriza *working progress* que también se ha visto acelerada y redimensionada por la aplicación de dispositivos *high tech* de vigilancia, sistemas avanzados en IA y *softwares* algorítmicos, tal y como muestra el volumen de proyectos pilotos financiados a nivel europeo (La Spina 2024, 178-179).

Partiendo de estas premisas y desde una aproximación crítica, este artículo busca analizar y reconstruir el proceso de metamorfosis hacia la frontera inteligente y poner así en evidencia su alcance ambivalente a la hora de reproducir ciertas “categorías migrantes estereotipadas de riesgo” en el control migratorio europeo. Para ello, se divide el trabajo en tres secciones. Después de la presente introducción, en la sección 2 se presenta una breve síntesis de la conceptualización y adjetivización de la llamada “frontera inteligente”. En la tercera sección, revisados los matices conceptuales y teóricos, se realiza un balance retrospectivo sobre la tecnificación de la frontera, remarcando su nueva morfología como complejo ecosistema digital y tecnológico, así como sus líneas de transformación futuras. Mientras que en la cuarta sección se reflexiona sobre por qué y cómo se activa mediante algunos ejemplos ilustrativos, la reproducción ilimitada de estereotipos y sus efectos discriminatorios indirectos para las personas migrantes.

## **2. La transformación inteligente de la frontera: génesis y alcance conceptual**

La invisibilidad de las fronteras inteligentes, en contraste con la visibilidad de los confines territoriales tradicionales, se caracteriza por el creciente proceso de digitalización y por el correlativo despliegue tecnológico y biométrico en las fronteras exteriores. Su alcance ha supuesto un incierto cambio de paradigma securitario, no solo porque plantea importantes retos a la hora de definir esta nueva frontera sino también desde un punto de vista doctrinal porque pone de manifiesto la controvertida e inexplorada naturaleza de estas fronteras en términos de inocuidad, certeza y objetividad (Taylor y Meissner 2020).

Desde su abordaje conceptual, la génesis de la voz *smart* es clave porque uno de sus componentes originales, la vigilancia biométrica fronteriza con fines de prevención, deriva directamente del control estratégico militar y de la seguridad perimetral implementada en el cruce fronterizo de los primeros países pioneros en tales sistemas (Nobile 2024, 289). Tal y como recuerda Méndez-Fierros (2023, 5), el concepto de fronteras inteligentes se encuentra por primera vez recogido en la *U.S.-Canada Smart Border Declaration* de 2001, y es fruto de un acuerdo entre los gobiernos de Estados Unidos y Canadá para crear una frontera segura que facilitara el libre flujo de personas y el comercio (Côté-Boucher 2008). En esta concreta latitud geográfica, las *smart borders* han estado en continua evolución (Brunet-Jailly 2006, Topak *et al.* 2015) intentando adecuarse a las nuevas formas de tecno-vigilancia fronteriza y control eficaz de las

amenazas de seguridad mediante la elaboración preventiva de perfiles para todas las categorías de viajeros y el mayor intercambio integrado de datos biométricos entre países.

En cambio, en el contexto europeo, la introducción de las *smart borders* se produce un decenio después, a partir de la Comunicación “Fronteras inteligentes - Opciones y camino a seguir” (CE- 2011)<sup>1</sup> y, en respuesta al incremento de flujos migratorios y al interés por reforzar la seguridad en las fronteras exteriores, al tiempo de facilitar el cruce para viajeros autorizados (Lehtonen y Aalto 2017). Su mayor concreción tecnonormativa no llegaría hasta los llamados *smart border packages* presentados por la Comisión en 2013 (Bigo *et al.* 2012, Jeandesboz *et al.* 2013, 14-15) y en 2016 respectivamente. La máxima de ambas propuestas era permitir un cruce de fronteras más fluido y rápido para la buena circulación de nacionales de terceros países cumpliendo así una “racionalidad biopolítica de lucha contra la inmigración irregular y de almacenamiento de la información” (Gäcke 2020, 263) en beneficio de los viajeros y de la economía de la UE” (CE 2016, 3). Así pues, en esta latitud geográfica, el apéndice *smart* ha abarcado la automatización de los pasos fronterizos, el registro en toda la UE de los datos de entrada y salida y el registro previo en internet de los viajeros sin visado de países no pertenecientes a la UE (Penasa 2022, 99).

Más allá de situar el origen de las *smart borders*, un aspecto siempre complejo ha sido delimitar el heterogéneo tejido morfológico de estos nuevos confines inteligentes (Nobile 2024, 291), así como elaborar un sencillo desglose técnico de sus diversos componentes o dispositivos. Para ello, se ha ido creando un amplio repertorio conceptual sobre el uso del llamado “tech package” en las fronteras (Nedelcu y Soysüren 2020, 1825) cuya inabarcable sofisticación técnica, se ha tratado de reducir con el uso de descriptores u adjetivos atribuibles a esta frontera. Así, por ejemplo, son varios los autores que se han referido predominantemente a este fenómeno transformativo utilizando el adjetivo más común y extendido de “smart” (Hayes y Vermeulen 2012), sin perjuicio de otras referencias o matizaciones semánticas como la de “big borders” por su alusión al manejo de “big data” y el concepto “bio-bordering” más representativo de los sistemas biométricos (Amelung y Machado 2019). En cambio, autores como Pötzsch (2018) han preferido hacer especial hincapié a la llamada tecnologización con su referencia al “iBorder/iBordering” frente a otros que potencian acepciones más amplias como la voz “digital borders” (Chouliaraki y Georgiou 2019) en un intento de englobar todas las tecnologías digitales, reservando la voz “high tech border” o “tecnofronteras” para aquellas más avanzadas dentro del proceso de *smartificación* (Arce Jiménez 2023 22). Esto es, admitiendo tanto la incorporación transversal de nuevas tecnologías de monitorización física (sensores, cámaras) como la aplicación de software algorítmicos, la biometría o la IA en los procedimientos administrativos y operacionales relacionados con dicho control.

En definitiva, estas diversas conceptualizaciones y adjetivaciones apuntadas subrayan, como sintetizan Oliveira Martins y Gabrielsen Jumbert (2022, 478), que las fronteras inteligentes son sistemas e infraestructuras integradas de tecnologías de la información y la comunicación (TIC) que involucran una combinación de dispositivos para el control

<sup>1</sup> Aunque la Comisión anunció por primera vez su intención de construir un Sistema Europeo de Entradas y Salidas en 2008 (CE 2008).

fronterizo (puertas electrónicas, quioscos de autoservicio, controles de seguridad automatizados, vigilancia fronteriza y software para pre-registro y evaluación de riesgos de los viajeros). Y al mismo tiempo, tal y como se analiza en la sección 3 bases de datos centralizadas con información a gran escala que abarcan desde permisos de viaje, historial de viajes e identificadores biométricos incluyendo huellas dactilares, rasgos faciales, emociones, etc.

### **3. Las *smart borders* como complejo ecosistema digital: una retrospectiva sobre el proceso de tecnificación de la frontera**

El régimen de cruce de fronteras exteriores del Espacio de Libertad, Seguridad y Justicia (ELSJ) se basa en dos criterios selectivos de control. Un “control mínimo” relacionado con la nacionalidad, que discrimina los titulares de la libre circulación dentro de la UE y un segundo control “exhaustivo” previsto para los ciudadanos de terceros países objeto de evaluaciones dinámicas (Sontowski 2018, Bellanova *et al.* 2022). Para ello, pese a un contexto tecno-normativo y programático cambiante (Tassinari 2022, Guild *et al.* 2025, 161), han sido creados seis sistemas TI de gran magnitud para implementar las políticas de la UE sobre fronteras, visados, cooperación policial y judicial penal, asilo y migración. Todos ellos persiguen un triple objetivo: garantizar un alto nivel de seguridad interior en un espacio Schengen de libre circulación, contrarrestar la inmigración irregular, la delincuencia transfronteriza y filtrar a las movilidades consideradas “de riesgo” (CE 2008, 2011). Así, desde su génesis, la tecnificación y digitalización de las fronteras exteriores europeas ha requerido y reclamado un marco dinámico de interoperabilidad para que los datos estuvieran interconectados (Bigo 2020, Cruz Ángeles 2020, 104) y que estos se pudieran integrar progresivamente con elementos de IA. Por ello, cabe detenerse, primero, en la fase de creación de estos sistemas y el marco de interoperabilidad (Broeders 2007, Vavoula 2021, Guild *et al.* 2025). Y, en segundo lugar, analizar las líneas de transformación futuras que plantea el Nuevo Pacto de Inmigración y asilo, y el nuevo Reglamento IA.

#### *3.1. Desde la creación de sistemas TI a gran escala hasta su interoperabilidad*

Bajo el nexo seguridad/facilitación en el cruce de las fronteras exteriores de la Unión Europea (Leese 2016) las primeras iniciativas de configuración de las *smart borders* en 2013 (Cruz Ángeles 2020, 339-341) preveían solamente un Programa de Registro de Viajeros (PRV) y un Sistema de Entradas/Salidas (SES). Esta primera propuesta embrionaria fue revisada (CE 2016) para acometer la reducción de la arquitectura del sistema informático al SES, así como incluir: un mecanismo de interoperabilidad entre el SES y el VIS; el uso de identificadores biométricos; el acceso a posibles antecedentes penales y/o delitos previos; los sistemas de autoservicio y puertas electrónicas; sin perjuicio de fijar garantías de protección de datos personales (Broeders 2011, Cruz Ángeles 2020). A partir de la nueva estrategia UE de Gestión Integrada de Fronteras, de forma gradual, junto a estos sistemas y tecnologías digitales se fueron incluyendo también por fases otros sistemas TI como el Sistema de Información Schengen (SIS); el Eurodac y el Sistema europeo de Información sobre Autorizaciones de viaje (SEIAV) sin perjuicio del Sistema Europeo de Información de Antecedentes Penales de Nacionales de Terceros Países (ECRIS-TCN). Todos ellos, bajo la supervisión de la Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos a Gran Escala en el



Espacio de Libertad, Seguridad y Justicia (eu-LISA) quién es la agencia encargada de regular sus componentes de interoperabilidad.<sup>2</sup>

Habida cuenta de su complejidad técnica y de lo inabarcable de su detallado análisis sistema a sistema, se pueden destacar una serie de características comunes (Guild *et al.* 2025, 166). En primer lugar, estos sistemas procesan principalmente datos personales de diferentes categorías de nacionales de terceros países, ya sean solicitantes de asilo, refugiados, migrantes irregulares, viajeros de corta estancia sujetos a requisitos de visado o viajeros sin visado y hasta delincuentes condenados. Los ciudadanos de la UE no están totalmente exentos, pero sus datos personales solo se procesan de forma incremental, por ejemplo, por la rama policial del SIS. En segundo lugar, la lógica compartida de todos ellos es desplegar un sistema específico y un canal de comunicación propio para cada tipología de viajero (sujeto a visado, exento de visado, solicitante de asilo), independientemente de las posibles redundancias o solapamientos entre sistemas. En tercer lugar, respecto a la información obtenida en relación con cada persona nacional de un tercer país, cada base de datos almacena y permite el tratamiento posterior de una amplia gama de datos personales (desde datos biográficos estándar o documentación de viaje hasta incluso datos biométricos con la única excepción de SEIAV que contiene una amplia variedad de datos alfanuméricos) en diversos foros y contextos; antes de su entrada, en las fronteras, en el territorio nacional y después de su salida. Todos los sistemas automáticos de identificación mediante impresiones dactilares, incluidos los utilizados actualmente para Eurodac, el VIS y el SIS, utilizan plantillas biométricas compuestas por los datos obtenidos mediante una extracción de características de muestras biométricas reales. Y, en cuarto lugar, atendiendo a los fines, estos son múltiples y divergentes, abarcando desde la modernización del control de la inmigración hasta la aplicación de la ley, por un mandato directo de seguridad o por un objetivo secundario de tener en cuenta los antecedentes penales o riesgos delictivos de las personas sometidas a valoración, como ocurre en los casos de Eurodac, SES, VIS y SEIAV. Ahora bien, dentro de este mínimo común denominador sí es posible delimitar algunas particularidades respecto a los fines y aplicación específica de estos sistemas TI a gran escala y los mecanismos de interoperabilidad derivados.

Dentro de los sistemas de información centralizados de la UE existentes para fronteras y seguridad, el SIS, siendo el primero de ellos y el más revisado, permite almacenar alertas sobre personas nacionales de terceros países a los que se les deniega la entrada o la estancia en el espacio Schengen o que son objeto de procedimientos de retorno. Si bien, con anterioridad a la reforma del 2018,<sup>3</sup> ya permitía a Europol y Eurojust acceder a

<sup>2</sup> Reglamento (UE) 2018/1726 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a la Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA) (DO L 295 de 21.11.2018).

<sup>3</sup> Véase versión consolidada con las modificaciones al Reglamento (UE) 2018/1860 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, sobre la utilización del Sistema de Información de Schengen para el retorno de nacionales de terceros países en situación irregular (DO L 312 de 7.12.2018); al Reglamento (UE) 2018/1861 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de las inspecciones fronterizas (DO L 312 de 7.12.2018); al Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal (DO L 312 de 7.12.2018).

descripciones y prever el almacenamiento de datos biométricos, es a partir del 2018 cuando la segunda generación del sistema (SIS II) incorpora la tecnología AFIS con huellas dactilares e imágenes faciales (Tassinari 2022, 669). Así, el sistema y su canal de comunicación SIRENE facilita el acceso a datos por autoridades policiales, judiciales y administrativas nacionales, así como agencias especializadas (Europol y Eurojust) y la consulta tanto de descripciones a efectos de denegación de entrada o de estancia en el espacio Schengen, así como sobre personas desaparecidas y sobre personas u objetos relacionados con infracciones penales. Tras su actualización en 2022<sup>4</sup> ya es posible recopilar información alfanumérica básica, así como datos biométricos (datos dactiloscópicos, impresiones palmares, imágenes faciales y archivos de ADN) y también las nuevas categorías de alertas pueden interrelacionarse.

Por otra parte, el Eurodac y su canal de comunicación Red Dublín (Guild *et al.* 2025, 164) es una base de datos europea que apoya a la aplicación de la legislación de la UE en materia de asilo y la lucha contra la entrada irregular de personas nacionales de terceros países.<sup>5</sup> Aunque entró en funcionamiento en 2003, este sistema se refundió en 2013 para permitir el acceso de autoridades policiales y Europol y, actualmente está todavía pendiente la entrada en vigor de la última reforma legislativa como se analizará en la sección 3.2. Este sistema prevé ya la recogida de las huellas dactilares de las personas solicitantes de asilo junto con el acceso a detalles sobre sus solicitudes, incluyendo información biográfica, imágenes faciales y copias de documentos de viaje con referencia a lugar y el momento en que se presentaron (Trauttmansdorff 2017, 113).

Siguiendo con esta cronología, el tercer sistema TI operativo desde 2011 es el VIS (Guild *et al.* 2025, 165) y aun cuando inicialmente contenía información sobre las solicitudes de visados de corta duración, permitiendo a los guardias fronterizos, las autoridades de inmigración y asilo así como las autoridades policiales y Europol verificar que una persona que presenta un visado es su titular legítimo e identificar que no se encuentra en territorio Schengen con documentos fraudulentos o sin ellos. Sus fines son de prevención, detección e investigación de delitos terroristas y penales. En 2021 fue revisado y actualizado<sup>6</sup> con vistas a ampliar este ámbito de aplicación (incluyendo datos sobre visados de larga duración y permisos de residencia) y mejorar los controles en la tramitación de visados (comprobaciones de antecedentes penales, entre otros). En

---

<sup>4</sup> Reglamento (UE) 2022/1190 del Parlamento Europeo y del Consejo de 6 de julio de 2022 por el que se modifica el Reglamento (UE) 2018/1862 en lo que respecta a la introducción en el Sistema de Información de Schengen (SIS) de descripciones de información en interés de la Unión relativas a nacionales de terceros países (DO L 185 12 de julio de 2022).

<sup>5</sup> Reglamento (UE) n° 604/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida (DO L 180 de 29.6.2013).

<sup>6</sup> Reglamento (UE) 2021/1133 del Parlamento Europeo y del Consejo de 7 de julio de 2021 por el que se modifican los Reglamentos (UE) núm. 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 y (UE) 2019/818 en lo que respecta al establecimiento de las condiciones para acceder a otros sistemas de información de la UE a efectos del Sistema de Información de Visados y Reglamento (UE) 2021/1134 del Parlamento Europeo y del Consejo de 7 de julio de 2021 por el que se modifican los Reglamentos (CE) núm. 767/2008, (CE) núm. 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 y (UE) 2019/1896 del Parlamento Europeo y del Consejo y por el que se derogan las Decisiones 2004/512/CE y 2008/633/JAI del Consejo, a fin de reformar el Sistema de Información de Visados (DO L 248, 13.7.2021).

general, el sistema almacena una amplia gama de datos personales, incluidas las huellas dactilares y las fotografías de todas las personas sujetas a los requisitos del VIS, incluso rebajando la edad a seis años. En cualquier caso, la mayor actualización del VIS es precisamente que los datos personales de las solicitudes de visado puedan ser objeto de comprobaciones automatizadas con otros sistemas TI a gran escala como ocurre con el SEIAV, incluyendo también bases de datos de Europol y SLTD y TDAWN de Interpol (Tassinari 2022, 669).

No obstante, entre los sistemas TI creados a partir del 2017, hay que diferenciar el alcance polivalente y más amplio de tres de ellos: SES, SEIAV y ECRIS-TCN. De un lado, el SES,<sup>7</sup> recientemente operativo desde octubre 2025, permite registrar la entrada y salida (y la denegación de entrada) de los titulares de visados de corta duración y de los viajeros exentos de visado, almacenando datos alfanuméricos, huellas dactilares y una imagen facial junto con documentos de viaje (Guild *et al.* 2025, 164) generando así una alerta por expiración de la duración máxima de estancia. Se trata de un sistema de información que se convertirá en la base de datos más amplia de almacenaje de datos biométricos. Su objetivo es mejorar la eficiencia y la automatización de los controles fronterizos; ayudar a identificar a los migrantes irregulares y quiénes han excedido el plazo de estancia; combatir así el fraude de identidad y documentos de viaje; y reforzar la seguridad interna permitiendo así bajo “un enfoque en cascada” (Tassinari 2022) que las autoridades policiales y Europol pueden acceder a los registros del historial de viajes para prevenir, detectar e investigar delitos de terrorismo u otros delitos graves.

Y, de otro lado, un punto de inflexión amerita el SEIAV,<sup>8</sup> el único sistema TI a gran escala que no contiene datos biométricos y está dirigido a nacionales de terceros países exentos de visado. Fue creado en 2018 pero aún no estará operativo hasta 2026. Sobre su naturaleza y alcance existe mucha controversia doctrinal, por ejemplo, entre ellos Guild *et al.* (2025, 168) han planteado dudas sobre la necesidad real de este nuevo sistema. No solo por los solapamientos parciales en términos de datos y finalidades perseguidas sino

<sup>7</sup> Reglamento (UE) 2017/2226 del Parlamento Europeo y del Consejo, de 30 de noviembre de 2017, por el que se establece un Sistema de Entradas y Salidas (SES) y se modifican el Convenio de aplicación del Acuerdo de Schengen y los Reglamentos (CE) núm. 767/2008 y (UE) núm. 1077/2011 DO L 327 de 9.12.2017. Reglamento (UE) 2017/2225 del Parlamento Europeo y del Consejo, de 30 de noviembre de 2017, por el que se modifica el Reglamento (UE) 2016/399 en lo que respecta a la utilización del Sistema de Entradas y Salidas (DO L 327 de 9.12.2017). Asimismo, una serie de actos de ejecución; Decisión (UE) 2018/1547; la Decisión (UE) 2018/1548; Decisión (UE) 2019/326; Decisión (UE) 2019/327; Decisión (UE) 2019/328. Reglamento de Ejecución (UE) 2022/1409 de la Comisión, de 18 de agosto de 2022 relativo a las normas detalladas sobre las condiciones de funcionamiento del servicio web y las normas de seguridad y protección de datos aplicables al servicio web, así como sobre medidas para el desarrollo y la ejecución técnica del servicio web, y por el que se deroga el Reglamento de Ejecución (UE) 2021/1224 (DO L 216 de 19.8.2022). Decisión de Ejecución (UE) 2022/1337 de la Comisión, de 28 de julio de 2022, por la que se establece el modelo para proporcionar información a los nacionales de terceros países sobre el tratamiento de datos personales en el Sistema de Entradas y Salidas (DO L 201 de 1.8.2022).

<sup>8</sup> Reglamento (UE) 2018/1240 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se establece un Sistema Europeo de Información y Autorización de Viajes (SEIAV) y por el que se modifican los Reglamentos (UE) 1077/2011, (UE) 515/2014, (UE) 2016/399, (UE) 2016/1624 y (UE) 2017/2226. DO L 236, 19.9.2018. Sin perjuicio de la legislación de modificación Reglamento (UE) 2021/1152 por el que se modifica el Reglamento (UE) 2018/1240, así como los Reglamentos (CE) 767/2008, (UE) 2017/2226, (UE) 2018/1861 y (UE) 2019/817 Reglamento (UE) 2021/1134 por el que se modifica el Reglamento (UE) 2018/1240, así como otros Reglamentos relacionados [Reglamentos (CE) 767/2008, (CE) 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 y (UE) 2019/1896].

incluso por la sujeción *tout court* de los ciudadanos de terceros países exentos de visado a otros sistemas TI a gran escala en el ELSJ (SIS, SES) así como al tratamiento derivado de las bases propias de los Estados miembros, las bases de datos de Europol y de Interpol, así como al tratamiento basado en los PNR para los viajeros aéreos. En concreto, este sistema exigirá a todos los viajeros exentos de visado que se dirijan al espacio Schengen que se sometan a un proceso de preselección para en caso de no detección de ninguna coincidencia obtener una autorización antes de su salida. La preselección y la concesión de la autorización se llevarán a cabo sobre la base de una verificación cruzada con: los datos almacenados en las bases de datos existentes de inmigración y fuerzas del orden; las normas de control que permiten la elaboración de perfiles basados en indicadores de riesgo; y una lista de vigilancia especial del SEIAV de personas sospechosas de haber participado en actos de terrorismo u otros delitos graves o respecto de las cuales existen indicios fácticos o motivos razonables para creer que cometerán tales delitos (San Martín Segura 2025). Para completar esta breve referencia a los seis sistemas, hay que añadir el sistema ECRIS-TCN creado en 2019 en el ámbito de la cooperación judicial penal. Este permitirá saber qué registros de otros Estados miembros poseen información sobre los antecedentes penales de nacionales de terceros países o apátridas, o de ciudadanos de la UE que también posean la nacionalidad de un tercer país, pero también podrá ser usado a efectos de inspección de seguridad en el nuevo procedimiento de triaje o screening (véase sección 3.2). Y, también almacenar datos biométricos y albergar datos alfanuméricos, pero por el momento no la identificación biométrica con imágenes faciales (Tassinari 2022, 670).

Ahora bien, paralelamente a la creación de sistemas TI de gran magnitud no se puede obviar que las *smart borders* también cuentan con una nueva arquitectura de gestión integral de identidades y de casos a partir de la adopción en 2019 del marco de interoperabilidad y su revisión en 2024.<sup>9</sup> Este paquete legislativo de interoperabilidad ha permitido no solo ampliar la comunicación e interconexión directa entre el sistema SEIAV (art. 11 Reglamento) y los otros sistemas informáticos junto a las bases de datos de las agencias de Europol e Interpol, sino también dar inicio a una fase potencial de *algoritmización* mediante la operatividad futura de sus diferentes componentes cruzados (Dumbrava 2021, 17, Tassinari 2025, Guild *et al.* 2025, 167). Por ejemplo, en síntesis, según el Reglamento de interoperabilidad, la funcionalidad técnica del Portal Europeo de Búsqueda (PEB) permite a las autoridades competentes consultar simultáneamente múltiples sistemas de información empleando datos biográficos como biométricos (Cap. II). Por una parte, el Servicio Compartido de Comparación Biométrica (SCB compartido) ya en vigor desde el 19 de mayo de 2025<sup>10</sup> genera y almacena las plantillas biométricas obtenidas a partir de todos los datos biométricos registrados en cada sistema subyacente (Cap. III) y las compara con los datos biométricos de los nuevos solicitantes para detectar

---

<sup>9</sup> Véase las modificaciones y referencia a estos componentes cruzados: el PEB y el RCDI en los art. 7.2, art. 17.1 y 4, art. 18.3, nuevo art. 20 bis, art. 24.1 2 bis y art. 24.5 a efectos de su utilización con la introducción del triaje de los nacionales de terceros países en las fronteras exteriores para el acceso al registro común de identidad de datos con fines de identificación o verificación, del Reglamento (UE) 2024/1352 que modifica los reglamentos (UE) 2019/816 y (UE) 2019/818 con el fin de introducir un proceso de “traje” para nacionales de terceros países en las fronteras exteriores de la UE (DO L, 2024/1352, 22.5.2024).

<sup>10</sup> Decisión de Ejecución (UE) 2025/875 de la Comisión, de 13 de mayo de 2025, por la que se determina la fecha de entrada en funcionamiento del servicio de correspondencia biométrica compartido con arreglo a los Reglamentos (UE) 2019/817 y (UE) 2019/818 (DO L, 2025/875, 14.5.2025).

posibles coincidencias (identificación biométrica) (Guild *et al.* 2025, 168). Por otra parte, el Repositorio Común de Identidad (RCDI) llevará a cabo una identificación más precisa en un archivo individual para cada persona registrada en los sistemas mencionados (excepto para el SIS) conteniendo tanto datos biométricos como biográficos, así como una referencia al sistema de obtención de los datos (Cap. IV). Mientras que, en apoyo del anterior, el Detector de identidades múltiples (DIM, podrá identificar si los datos de identidad biográficos existen en otros sistemas, detectando posibles identidades múltiples vinculadas al mismo conjunto de datos biométricos (Cap. V). Y, por último, el Repositorio Común de Informes y Estadísticas (RCIE) proporcionará datos estadísticos y el suministro de informes personalizables para el análisis y la especificación de perfiles de riesgo que se utilizarán posteriormente para la investigación previa de las personas solicitantes de visado y con exención de visado (art. 39).

### 3.2. *Las líneas de transformación futuras de las Smart borders: el Nuevo Pacto europeo de migración y asilo<sup>11</sup> y el Reglamento IA*

Si bien la estructura morfológica de las *smart borders* europeas ya ha quedado casi configurada por estos sistemas TI a gran escala dentro de este marco de interoperabilidad, realmente aún queda por saber cómo se transformará su nueva dimensión de sobrevigilancia algorítmica y biométrica (Alonso Tomé 2025) tanto para acciones materiales como de apoyo formal a la toma de decisiones. De hecho, en el caso del SEIAV y el VIS, son varios los autores que indican que no se trata de mero software auxiliar, sino de una auténtica “tecnología normativa” con efectos jurídicos en la toma de decisiones (Velasco Rico y Laukyte 2024, Guild *et al.* 2025). De ahí que su complejidad técnica y su interoperabilidad anidada (San Martín Segura 2025, 565), las hacen diferentes al resto de sistemas al abarcar el procesamiento automatizado y la evaluación de las solicitudes individuales, así como la emisión de autorizaciones de viaje o visado. Además, su interconexión con las infraestructuras fronterizas nacionales, utilizando la infraestructura de hardware y software existente proporcionada por el SES, garantiza su plena e integral interoperabilidad con el resto de sistemas. De hecho, los principales analistas técnicos del sistema SEIAV han asumido en general que es cuestión de tiempo que se incorporarán capacidades de aprendizaje automático y, por consiguiente, una nueva forma de discrecionalidad algorítmica a partir de la especificación previa de riesgos (Musco Eklund 2023).

Precisamente por ello, entre las líneas de transformación futuras de las *smart borders* hay que tener en cuenta el punto de inflexión que produce el Nuevo Pacto europeo sobre Migración y Asilo 2020, adoptado el 14 de mayo de 2024, con las reformas legislativas que se introducen en el sistema de triaje, por medio de los sistemas SES y SEIAV, así como la activación de otros componentes cruzados. Con la aplicación a nivel nacional de estas reformas legislativas, estos sistemas recopilarán en bloque los datos personales, se intercambiarán entre las fuerzas policiales de toda la UE, así como se utilizarán ya sistemas de identificación biométrica para rastrear los movimientos de las personas

---

<sup>11</sup> Comunicación de la Comisión al Parlamento Europeo al Consejo, al Comité económico y social europeo y al Comité de Regiones, relativa al Nuevo Pacto sobre Migración y asilo (Bruselas 23 de septiembre 2020, COM (2020) 609 final).

migrantes indocumentadas (CE 2022), reforzando así las prácticas de identificación integral de los nacionales de terceros países y su rápida clasificación o categorización.

En particular, su incidencia va a ser ambivalente, por ejemplo, en los procedimientos de control y los procedimientos fronterizos de nueva creación del Reglamento *Screening*.<sup>12</sup> Este reglamento admite el cribado o triaje por medio de diversos controles de identidad, salud y seguridad de todas las personas que según el art. 1 “estén a punto de entrar en el espacio Schengen” con la finalidad aparentemente neutra y operativa de “remitirlas a los procedimientos adecuados”. Básicamente se articula un primer control previo (traje) a la entrada para (casi) cualquier persona que llegue a una frontera de la UE, sin cumplir las condiciones de entrada o para aquellas que sean desembarcadas tras una operación de búsqueda y salvamento. Y, una segunda fase, en la que se activan tras la identificación de cada situación, los respectivos procedimientos de asilo rápido en frontera o de devolución en instalaciones fronterizas o en la proximidad de las mismas. En función de los resultados de la identificación, si no existe una base legal para la entrada, la persona migrante será transferida al procedimiento de retorno rápido. Si en cambio la persona ha solicitado asilo y se considera que no representa una amenaza para la seguridad o si hay minoría de edad será transferida al sistema de asilo ordinario, pero si la probabilidad de reconocimiento es baja, se le remite a un procedimiento acelerado según el Reglamento sobre procedimientos de asilo,<sup>13</sup> y, en caso de denegación, a un procedimiento de retorno rápido conforme a lo dispuesto en el art. 4.5 del Reglamento sobre procedimientos fronterizos de retorno.<sup>14</sup> Por lo tanto, el objetivo del cribado es identificar a las personas migrantes y verificar que no representan una amenaza para la seguridad interior u orden público, pero también incluir controles sanitarios para identificar a las personas vulnerables que necesiten atención sanitaria o que sean una amenaza para la salud pública.

Según el Reglamento *screening*, estos procedimientos de cribado o triaje requerirán que los datos personales y biométricos de cada persona (art. 8.5 y art. 14) que entre en la UE se cotejen con múltiples bases de datos policiales y de inmigración nacionales y europeas, así como con sistemas gestionados por Europol e Interpol (art. 16). A tal propósito, las modificaciones al Reglamento 2024/1352 para la introducción del triaje fijan que la verificación a efectos de seguridad debe llevarse a cabo en los mismos sistemas que los usados para los solicitantes de visados o de autorizaciones de viaje con arreglo al SEIAV y, en concreto debe permitir el acceso a las autoridades competentes al ECRIS-TCN en lo que respecta a las personas condenadas por delitos de terrorismo u otros delitos graves (art.2.2). Se introducen cambios en el art. 17 para crear vía componente cruzado RCDI un expediente individual para cada persona registrada en el SES, el VIS, el SEIAV, Eurodac o el ECRIS-TCN, con el fin de facilitar la identificación

---

<sup>12</sup> Reglamento (UE) 2024/1356 del Parlamento Europeo y del Consejo, de 14 de mayo de 2024, por el que se introduce el triaje de los nacionales de terceros países en las fronteras exteriores y se modifican los Reglamentos (CE) n. 767/2008, (UE) 2017/2226, (UE) 2018/1240 y (UE) 2019/817 (DO L, 2024/1356, 22.5.2024).

<sup>13</sup> Reglamento UE 2024/1348 del Parlamento Europeo y del Consejo, de 14 de mayo de 2024, por el que se establece un procedimiento común en materia de protección internacional en la Unión y se deroga la Directiva 2013/32/UE (DO L, 2024/1348, 22.5.2024).

<sup>14</sup> Reglamento UE 2024/1349 del Parlamento Europeo y del Consejo, de 14 de mayo de 2024, por el que se establece un procedimiento fronterizo de retorno y se modifica el Reglamento (UE) 2021/1148 (DO L, 2024/1349, 22.5.2024).

correcta o la verificación de la identidad de las personas registradas en tales sistemas según arts. 20 y 20 bis). Todo ello sin perjuicio de apoyar el funcionamiento del DIM, de conformidad con el art. 21, y racionalizar el acceso por parte de las autoridades designadas y de Europol a los mencionados sistemas, con fines de prevención, detección o investigación criminal. Las autoridades de triaje, tal como se definen en el art. 2.10 tendrán derecho a acceder a los datos del ECRIS-TCN y a consultarlos utilizando el componente cruzado PEB previsto en el art. 6 del Reglamento de interoperabilidad.

Asimismo, en el contexto de los procedimientos de asilo, se permitirán prácticas tecnológicas intrusivas en varias fases de la tramitación del asilo, inclusive un aumento de los registros de objetos personales, allanando así el camino a prácticas invasivas como la extracción de datos de teléfonos móviles o dispositivos electrónicos personales (Scheel 2024, Josipovic 2024) para encontrar pruebas que permitan evaluar la veracidad de sus solicitudes o comprobar su identidad, edad o país de origen (considerando 22). En cualquier caso, el nuevo Reglamento sobre procedimientos de asilo también permite el uso de entrevistas a distancia y videoconferencias para las personas detenidas y durante el procedimiento de recurso (art. 14) afectando así negativamente a la calidad y la equidad de los procedimientos para los sujetos en situaciones más vulnerables (Jasmontaite-Zaniewicz y Zomignani Barboza 2021).

Simultáneamente, para agilizar la movilidad del “solicitante de asilo genuino”, a la luz de los cambios recogidos en el Reglamento Eurodac,<sup>15</sup> con su entrada en vigor será obligatoria la recogida sistemática de datos biométricos de las personas solicitantes de asilo, que se conservarán en bases de datos masivas hasta diez años. Las mismas se intercambiarán en cada paso del proceso migratorio y serán accesibles a las fuerzas policiales de toda la UE con fines de seguimiento y control de identidad. Incluso, será posible incluir la recogida de datos alfanuméricos de identidad que permitan el recuento de personas solicitantes de asilo (no solo de solicitudes); la inclusión de nuevas categorías de personas (aquellas desembarcadas tras operaciones de búsqueda y rescate para un control preliminar en frontera); el tratamiento de nuevos datos biométricos (imagen facial y ADN); así como la reducción de la edad para la toma de huellas dactilares (de los 12 a los 6 años). Y, figuran entre las reformas del Reglamento (UE) 2024/1358 que el sistema se utilizará para fines adicionales relacionados con la migración, tales como el reasentamiento y los retornos conforme a su considerando 4. Para ello, se añade como garantía que los datos biométricos de las personas registradas con objeto de tramitar un procedimiento de admisión deben conservarse en Eurodac tan pronto como se conceda el estatuto, y a más tardar, en las 72 horas siguientes. Y, en su considerando 12, se explicita que la identificación biométrica constituye un elemento importante para determinar la identidad exacta, pues garantiza un nivel muy elevado de precisión en la identificación.

Junto a estas reformas legislativas promovidas por el Pacto europeo hay otros cambios normativos que tienen una clara incidencia en la transformación inteligente de la

---

<sup>15</sup> Reglamento UE 2024/1358 del Parlamento Europeo y del Consejo, de 14 de mayo de 2024, sobre la creación del sistema «Eurodac» para la comparación de datos biométricos a efectos de la aplicación efectiva de los Reglamentos (UE) 2024/1351 y (UE) 2024/1358 (DO L, 2024/1350, 22.5.2024).

frontera, como es la reciente reforma en 2024 del Código de Fronteras Schengen.<sup>16</sup> Esta permite generalizar los controles policiales con fines de control de la inmigración, facilitando así la práctica de perfiles raciales en el territorio de la UE tanto en las fronteras interiores como en las exteriores. Por ejemplo, los sistemas generalizados de control fronterizo automatizado (ABC), las puertas electrónicas o de otras tecnologías como drones, sensores de movimiento, cámaras termográficas se usan no solo para la identificación de las personas que cruzan las fronteras antes de su llegada sino incluso para facilitar las devoluciones o deportaciones (Vrăbiescu 2022).<sup>17</sup>

A pesar de las críticas ya vertidas por la doctrina sobre la discrecionalidad algorítmica del sistema SEIAV o incluso sus imbricaciones penales (Michéa y Rousvoal 2021, Derave *et al.* 2022), la progresiva irrupción de sistemas IA de aprendizaje-máquina abre otro escenario inédito de metamorfosis de la frontera europea (Kilpatrick y Jones 2022, 31-46). Este escenario en algunos países como Alemania, Suecia o Dinamarca (Guild *et al.* 2025, 194) ha derivado ya en la generación de contenidos, predicciones, recomendaciones o decisiones con capacidad de inferencia para la evaluación automatizada de riesgos, la predicción por medio de polígrafos y vigilancia por drones, cámaras termográficas, sensores de movimiento y térmicos o bien los sistemas de identificación y categorización biométrica en remoto,<sup>18</sup> la captación y reconocimiento de imágenes faciales, emociones, idiomas;<sup>19</sup> o la recopilación automática de huellas dactilares u otros datos personales (CE 2020, 2021, Burgess y Kloza 2021, EDRi-European Digital Rights 2022, Musco Eklund 2023, 250). De igual modo, la Agencia Europea de la Guardia Fronteras y Costas<sup>20</sup> utiliza una serie de tecnologías fronterizas automatizadas encubiertas como drones de vigilancia con una impresionante capacidad de procesamiento de datos a través de estrategias fronterizas y de vigilancia altamente tecnificadas para proteger contra los riesgos asociados a la migración irregular (art. 10.1 x). Y, cuando participa en operaciones conjuntas, retorno, pilotajes, intervenciones, etc., puede procesar ciertos datos de personas que cruzan fronteras sin autorización de viaje (art. 88). Aunque directamente no “tome” la biometría por si misma, puede actuar sobre datos biométricos interoperables que formen parte del SIS, SES, VIS o Eurodac, lo que ya implica verificación cruzada de identidades y comparaciones masivas que podrían generar sesgos o usos “profiling-like”.

---

<sup>16</sup> Reglamento (UE) 2024/1717 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, que modifica el Reglamento (UE) 2016/399 por el que se establece un Código de normas de la Unión para el cruce de personas por las fronteras (DO L 2024/1717, de 20.06.2024).

<sup>17</sup> Véase considerando 16 “los medios técnicos para impedir los cruces no autorizados de la frontera podrían incluir tecnologías modernas, como drones y sensores de movimiento, así como unidades móviles y, cuando proceda, todo tipo de infraestructuras fijas y móviles. El uso (...) tiene que basarse en disposiciones claramente definidas del Derecho nacional y ejercerse de conformidad con ellas. Y, el considerando 21 sobre las fronteras interiores.

<sup>18</sup> Por ejemplo, el proyecto ROBORDER incluye un sistema de vigilancia fronteriza con capacidad robótica mediante vehículos aéreos, de superficie submarinos y terrestres.

<sup>19</sup> Entre otros, iBorderCTRL, TRESPASS o AVATAR, un sistema virtual automatizado para la evaluación de la verdad en tiempo real (Dumbrava 2021, CE 2021, Romano 2023) y sistemas de reconocimiento del habla (EMN-European Migration Network 2022, 10-11).

<sup>20</sup> Considerando 35 y 48 Reglamento (UE) 2019/1896 del Parlamento europeo y del consejo de 13 de noviembre de 2019 sobre la Guardia Europea de Fronteras y Costas y por el que se derogan los Reglamentos (UE) 1052/2013 y (UE) 2016/1624.



Por todo ello y en último lugar, otro aspecto que no debe obviarse como línea de transformación a futuro es el Reglamento de IA.<sup>21</sup> Con ello, será más controvertida la posible afectación que tendrán los sistemas preexistentes TI a gran escala con algunas prácticas de IA de alto riesgo prohibidas vía art. 5 (entre otros, manipulación subliminal engañosa, *scoring* social, biocategorización, etc). Y, no solo eso, quizás no sean suficientes estos niveles de protección ante la imprevisibilidad del despliegue inevitable de la IA en la elaboración de perfiles algorítmicos, así como el posible tratamiento casi integral de datos biométricos, concretamente huellas dactilares (o datos dactiloscópicos) e imágenes faciales (Cruz Ángeles 2022). Por el momento, se desconoce si los sistemas TI y los componentes de interoperabilidad funcionarán basándose en la IA o no, ni dónde y en qué medida lo harán dada la falta de referencia explícita a la IA en sus regulaciones. Por este motivo, a la luz de las numerosas voces críticas aquí referenciadas (San Martín Segura 2025, Guild *et al.* 2025) se insiste en que ni el SEIAV ni el VIS abordan suficientemente los requisitos y garantías especiales que deben proyectarse sobre el proceso de construcción de sus modelos algorítmicos. Y, en este sentido, por ejemplo, Guild *et al.* (2025, 217) reiteran sus dudas, sobre el componente cruzado RCIE, ya que recopilará y almacenará (entre otros) datos estadísticos del VIS, el SES y el SEIAV sobre personas nacionales de terceros estados que han excedido el plazo de estancia y, por tanto, procesarán de forma integral información relativa a la denegación de entrada, así como podrán realizar una trazabilidad panorámica y una verificación cruzada integral sobre la evolución específica del riesgo de dicha movilidad no deseada.

A día de hoy no existe aparente contradicción con los niveles de protección que marca el Reglamento de IA y el blindaje existente sobre los sistemas de TI a gran escala del Anexo X tratados como de alto riesgo, con obligaciones estrictas para proteger derechos. De ahí que cabe cuestionarse abiertamente si en la fecha límite del cumplimiento de adecuación a estos criterios se ampliará de forma dinámica las prohibiciones que rigen en el ámbito de la gestión y control fronterizo migratoria a todos los posibles impactos negativos asociados a la IA o, por contra si excepcionará *in extremis* estos sistemas TI a gran escala en funcionamiento o en servicio antes de agosto del 2027. Es decir, por cumplir el objetivo europeo de apuesta fiable de la IA y por ser “medios” necesarios e indispensables para alcanzar los fines legalmente previstos (La Spina 2024, 183-187, Tassinari 2025, 363).

#### **4. Hacia la reproducción ilimitada e invisible de categorías migrantes estereotipadas a través de las *smart borders***

Habida cuenta del alcance potencial de las transformaciones estructurales de las fronteras en contextos migratorios, las *smart borders* son presentadas equívocamente desde el *tecnosolucionismo* de forma inocua como exponentes eficientes para hallar una respuesta excepcional a una amenaza a la seguridad permanente respecto a quiénes están en los márgenes de la libre circulación. El aumento de los flujos migratorios globales supone un reto-pretexto para reforzar la capacidad de las autoridades para definir y diferenciar la movilidad deseada porque pone en primer plano la necesidad de clasificación y categorización de las personas migrantes (Taylor y Meissner 2020, 275).

---

<sup>21</sup> Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (DO L, 2024/1689, 12.7.2024).

Por lo tanto, si bien las *smart borders* son más que la simple fortificación material y visible del confín territorial (Velasco 2022), tal y como sostiene San Martín Segura (2019, 34), su devenir en inteligente se dirige a renovar y agilizar de forma exponencial “la capacidad de registro y procesamiento de información (...) e incluso automatización” de esta. Básicamente, por su gran capacidad de almacenamiento y, posterior procesamiento de los datos personales de diferentes grupos de nacionales de terceros países, así como gracias a su sofisticada infraestructura de comunicación. Además, porque el acceso y consulta de estos sistemas abarca una amplia gama de entidades beneficiarias: autoridades nacionales y algunas agencias de la UE, como la Agencia europea de Fronteras y Costas (Frontex), Europol o la Agencia de la Unión Europea para el Asilo en cumplimiento de sus finalidades.

Es así como esta tecnificación de las fronteras exteriores se hace imprescindible e inevitable por su esperada capacidad de identificación de una amenaza para la seguridad, y en la medida que se convierten en dispositivos socio-técnicos de individualización de los riesgos, de selección preventiva y de creación de una serie de identidades diferenciales, “entre viajeros de buena fe y viajeros de riesgo” (Campesi (2012, 16) readaptando así la lógica selectiva del *risk profiling* de Harcourt (2007). Sin embargo, como bien recuerda San Martín Segura (2025, 577) esta categorización no es en absoluto novedosa. El control fronterizo ha funcionado tradicionalmente utilizando “listas de viajeros indeseables sujetos a prohibición (...) de viajeros de confianza sujetos a controles mínimos y “listas de control de forma más flexible en función del grado de sospecha”.

En cualquier caso, el potencial del despliegue de los sistemas y componentes cruzados de las llamadas *smart borders* (Nobile 2024, 290), sí es más cuestionable por su dudosa capacidad de identificación neutral, transparente y no discriminatoria incluso cuando existen razones de seguridad y de control efectivo de “poblaciones sospechosas” o “grupos de riesgo”. Básicamente porque las *smart borders* no solamente contribuyen a realizar reproducciones del confín de forma potencialmente indefinida y arbitraria (Vaughan-Williams 2009, 734) sino porque estas formas favorecen, por medio de la desconexión territorial, zonas permanentes de extraterritorialidad jurídica y de reificación para un colectivo “diana” como son las personas migrantes y sus derechos (Campesi 2012); con la ayuda de dinámicas continuas de rápida categorización (Taylor y Meissner 2020, 275). Así pues, aunque la aplicación del paquete de medidas sobre fronteras inteligentes crea y mantiene registros electrónicos de todos los viajeros nacionales de terceros países que entran en el espacio Schengen (Jeandesboz 2016, 293), su modo de funcionamiento interoperable excede el de un simple sistema de sobrevigilancia masiva de datos o de un mecanismo de clasificación económica en nombre de la seguridad (Leese 2016). De hecho, cada vez hay más indicios claros que las conviertan en *digital racial borders* por sus lógicas de degradación social y exclusión (De Genova 2013, Achiume 2022) por su asociación rápida con el recurrente trinomio: irregularidad, delincuencia o terrorismo. De hecho, el alcance o efecto menos explorado de las fronteras inteligentes, según San Martín Segura (2025, 567) es la “capacidad de anamorfosis de ciertas categorías jurídicas migrantes”. En concreto, es ilustrativo en algunos sistemas TI a gran escala como el VIS y el SEIAV donde se aplica un efecto de distorsión y un enfoque sesgado/alterado de esas movilidades solicitantes. Por lo tanto, nada garantiza en su marco normativo que se pueda evitar ni controlar un efecto de

exacerbación, validación estadística, duplicación y nueva reproducción de categorías estereotipadas consideradas desviadas por no corresponder con la categoría jurídica ideal-tipo deseada “migración ordenada y *bona fide*”.

En este sentido, de acuerdo con Ghidoni y Morondo (2023), un daño distintivo en la reproducción de los estereotipos o categorías migrantes estereotipadas (Cook y Cusack 2010, 19) reside en su capacidad para borrar la identidad individual y las características específicas del sujeto, facilitando sin más la toma de decisiones basadas en rasgos grupales asumidos. Se denomina este efecto “serialización”, porque los individuos, en este caso las personas migrantes son tratadas como entidades intercambiables dentro de una serie de idénticas que pierden su condición de sujetos autónomos, quedando así subsumidos en la homogeneidad de características o riesgos generales de su grupo/categoría tipo. Este mismo proceso de estereotipización se reproduce en las fronteras inteligentes dando lugar a una discriminación indirecta y a una presunción genérica de un comportamiento desviado que puede producir diferentes efectos o alcances según el nivel de discrecionalidad en el procesamiento algorítmico de las categorías de datos obtenidos de los sistemas existentes o incluso subyacentes.

A modo de ejemplo, tal y como detalla San Martín Segura (2025, 555 y 566), respecto al SEIAV, pero también aplicable al VIS, esto ocurre cuando se categoriza un nacional de un tercer país como potencialmente peligroso por presentar rasgos característicos de una categoría determinada y no por haber sido individuado como autor de un acto concreto. Precisamente, el procesamiento “orientado al futuro” del SEIAV se produce cuando se inducen posibles comportamientos futuros a partir de correlaciones estadísticas, que se basan en una lógica de riesgo futuro. Esta atribución derivada del procesamiento orientado al futuro y del conductismo de datos, según Gäckle (2020, 267) “reproduce un régimen de verdad estadística” que crea, por tanto, “nuevas inmovilidades en forma de exclusiones justificadas en base a acciones no realizadas todavía”. No en vano, los indicadores de riesgo del SEIAV y su secuencia de definición parte de determinada información previamente tratada por la Comisión (art.33.2 Reglamento SEIAV) sobre las estadísticas generadas por el funcionamiento del SES (índices anormales de estancias prolongadas y denegaciones de entrada para determinados grupos de viajeros) y del propio SEIAV (índices anormales de denegaciones de autorizaciones de viaje debido a las tres fuentes de riesgo para grupos específicos y correlaciones entre los datos de los formularios de solicitud y los resultados observados posteriormente); y pruebas aportadas por los Estados miembros en estas diferentes dimensiones de riesgos sobre determinados grupos de viajeros y, en el caso de los riesgos epidémicos, también por organizaciones sanitarias (ECDC, OMS). Como resultado esperado, la población migrante emerge así como una “categoría o representación estadística” (Bigo 2011, 99) de la cual se derivan formas estereotipadas y de verdad sobre la noción de riesgo. Se hace, por tanto, inevitable la vinculación o asociación entre los fenómenos colectivos/grupales con esos rasgos individuales calculables y una serie “idéntica” de riesgos potenciales (Foucault 2008, 60).

De este modo, se obtiene un conjunto de características de grupos específicos de viajeros asociados a estos riesgos comunes y, en última instancia el procesamiento automatizado permite la reasignación de los recursos de control a las personas “de riesgo” antes de su salida, y se justifica un *laissez-faire, laissez passer* solo en el control de los viajeros con

perfiles de “bajo riesgo”. Con ello, directamente e indirectamente, se generan graves problemas de discriminación, pues tal y como sostiene Blasi Casagran (2021, 452-454), los controles de identidad migratoria *tout court* facilitados por la interoperabilidad son intrínsecamente discriminatorios *per se*, ya que implican un trato diferenciado entre los ciudadanos de la UE y los nacionales de terceros países, así como la suposición estadística de que estos últimos son más propensos a participar en actividades que amenazan al orden público. De hecho, Guild *et al.* (2025) no descartan que se podría permitir a las autoridades nacionales emprender investigaciones indiscriminadas, ya que no existe un catálogo equivalente a escala de la UE de registros sobre los ciudadanos de la UE ni se cuenta por ahora con tal volumen de información sobre su movilidad o comportamiento. Además, no es un aspecto menor, según Gäckle (2020, 262) la ausencia de procesos de subjetivación en estas prácticas de control (en comparación con las prácticas disciplinarias o humanas) y, la consiguiente serialización de idénticas categorías, dan como resultado una categorización más dinámica (Dijstelbloem y Broeders 2015, 21) y, más sesgada de los viajeros. Hay una alta probabilidad que determinados grupos de viajeros no deseados se vean en desventaja en comparación con otros, sin contar con el agravante de que tales categorías no deseadas o sospechosas en el ámbito de la inmigración ya estén entrelazadas con estereotipos sociales, raciales y étnicos (San Martín Segura 2025, 566), abocados a un círculo vicioso o espiral sin posibilidad de resistencia.

Sin embargo, este efecto de serialización o reproducción ilimitada de categorías estereotipadas sobre la movilidad deseada y no deseada se podría reforzar si se produce una fase de mayor tecnificación IA de las *smart borders* porque en un nivel básico, aquellos sistemas TI a gran escala que incorporan datos biométricos como Eurodac VIS y SIS con la excepción del SEIAV, tratarán diferentes tipos de datos biométricos, haciendo hincapié en la verificación y la identificación inicialmente a través de huellas dactilares y, más recientemente, de imágenes faciales, con excepción del ECRIS-TCN. Asimismo, si pueden generar plantillas biométricas de los componentes cruzados (RCDI o DIM), se podrían utilizar para vincular o identificar las características particulares seleccionadas por el algoritmo; en un nivel más complejo, no se descarta en un futuro que la información biométrica recopilada podría permitir a estos sistemas y personal fronterizos extraer conclusiones procesables o estadísticas vía RCIE sobre tales datos. Y, finalmente la automatización o la introducción de la IA para la toma de decisiones, incluso con fines específicos, proporcionados y no discriminatorios podría permitir combinar la biometría y la vigilancia de datos con formas de análisis basadas en algoritmos (Pötzsch 2015, 108) objetivando y normalizando así sus efectos discriminatorios por ser estos inevitables o imperceptibles.

De hecho, por ejemplo, cabe la posibilidad de utilizar herramientas de IA para mejorar la identificación de riesgos para grupos específicos de viajeros mediante la identificación de patrones o un conjunto de características comunes a partir del análisis de datos históricos en el RCIE relacionados con la seguridad, la migración irregular y los altos riesgos epidémicos. Así pues, es probable que el RCIE utilice herramientas de IA en la recopilación de datos estadísticos anonimizados y análisis personalizados e “intersistémicos” con fines políticos y operativos. El resultado será que el RCIE no estará sujeto a ninguna supervisión, ni desde la perspectiva de la legislación de la UE en materia de protección de datos ni del Reglamento de IA hasta 2030 (inclusive sus

prórrogas o excepciones) simplemente dada la no aplicabilidad del Reglamento IA durante ese periodo de tiempo. Y, todo ello, anticipa que así será presumiblemente, habida cuenta del poder y supervisión discrecional otorgado a la Agencia eu-LISA y a la Agencia Europea de la Guardia Fronteras y Costas en el plano operacional de sus misiones, así como por los importantes obstáculos que encuentran las personas para recurrir a la vía judicial para garantizar sus derechos o el tratamiento de datos sin comprometer o dilatar la viabilidad de los procesos en curso de autorización de entrada (arts. 37.3, 40.3, 41.7 Reglamento SEIAV) o de expedición de visado (art. 32 y ss Reglamento VIS), entre otros.

Por consiguiente, la transformación inteligente de las fronteras exteriores de la UE y el despliegue tecnológico de sistemas basados en IA (Molnar 2023, 309) es un punto de no retorno que puede contribuir con mayor celeridad al etiquetado social y algorítmico de las personas migrantes bajo el pretexto de la seguridad, el miedo y la desconfianza (Romano 2023, 242). Esta posibilidad y su relación práctica, tal y como se ha recordado desde estudios sobre la discriminación algorítmica (Vantin 2021, Musco Eklund 2023) no puede ser contrarrestada de forma efectiva y garantista, pues nada impide que se pueda discriminar de forma indirecta o por aproximación (*proxies*), incluso si no hay datos sensibles para elaborar “indicadores de riesgo”. Tal y como se ha explicado mayormente respecto al SEIAV y en menor medida del esquema de especificación de riesgos adoptado en el VIS mediante el art. 9, letra j), de su Reglamento. Al igual que los otros cuatros sistemas TI a gran escala cuyo objetivo principal no es la investigación criminal (SIS; SES, Eurodac), ambos son mecanismos de control digital de los movimientos fronterizos basados en un tipo específico de clasificación estática de la movilidad fronteriza que permite una gobernanza “dinámica” del tránsito fronterizo gracias al régimen de interoperabilidad anidado que contienen. Ambos sistemas fueron concebidos como una plataforma para la emisión automática de autorizaciones de viaje o expedición de visado que arrojen un resultado positivo (CE 2016, 10), pero no hay precedentes sobre esta forma sofisticada de “extracción y perfilado de datos personales, inclusive biométricos en el caso del VIS” (Guild *et al.* 2025, 176) ni tampoco sobre las “correlaciones entre la información recopilada mediante el formulario de solicitud y la permanencia irregular o denegaciones de entrada”. Así pues, la serialización de categorías estereotipadas de riesgo grupal no puede evitarse o limitarse ni tampoco controlar sus efectos discriminatorios indirectos. Por ejemplo, el sexo puede indicar por *aproximación* la orientación sexual; la ciudad de residencia puede revelar la etnia y el color; el nivel de estudios y la ocupación indicarán la propiedad y la afiliación sindical; la nacionalidad podría ser un indicador indirecto de origen étnico o religión, etc. (Vavoula 2021). Adicionalmente, en otro orden de cosas, el Reglamento SEIAV confía a la Agencia de Fronteras y Costas la especificación definitiva de los indicadores de riesgo, proporcionando únicamente la información en la que debe basarse en la elaboración de perfiles mediante la comparación de los indicadores de riesgo específico con los datos del expediente de solicitud (art. 33.4 Reglamento SEIAV). Aunque su objetivo es un cálculo de riesgo automatizado y cuantitativo como núcleo algorítmico del sistema, dispositivos como el SEIAV admiten la discrecionalidad técnica de la Agencia eu-LISA al considerar como “ruido” (*noise data*) las correlaciones y sesgos que arrojan tales sistemas si tienen acceso o manejan información a gran escala sobre los flujos migratorios no deseados. No solo se sigue una lógica de verificación cruzada con bases de datos, sino

que se difumina la distinción entre ciertas categorías al someter a todas las personas solicitantes de acceso a una evaluación de riesgos tipificados y al permitir que un algoritmo (no especificado en el Reglamento) proporcione el perfil de riesgo atribuido mediante la verificación cruzada (potencialmente integral) de la información personal del viajero con indicadores de riesgo específicos y estáticos.

De igual modo, según San Martín Segura (2025, 580), el pronóstico negativo de tales sistemas evoca con laxitud la noción de peligrosidad social y, en definitiva, amplifica los estereotipos ya asumidos en torno a la inmigración integrados en el diseño normativo y en el resultado analítico de ambas agencias al perfilar su funcionamiento operativo. La morfología de las *smart borders* permite así una nueva categorización prospectiva de la población migrante cada vez más modulada o capilar (San Martín Segura 2019, 26 y 27) atendiendo a un riesgo abordado como una entidad esencialmente cualitativa desde perspectivas sociales sesgadas, aun cuando se insista que parte de una especificación cuantitativa y estandarizada en la evaluación de riesgos. El resultado esperado es una categorización radicada inevitablemente en la presunta veracidad u objetividad estadística de esos estereotipos que no alejan sus efectos discriminatorios indirectos, sino que privan a las personas migrantes de todo “espacio de legalidad o confianza” (Epstein 2007, De Genova 2013).

## 5. Reflexiones finales

Las *smart borders* ejemplifican a la perfección el alcance de la portabilidad y desterritorialización de los confines territoriales por medio de la implementación de herramientas o dispositivos tecnológicos basados tanto en sistemas de información como en softwares avanzados muy dispares entre sí. El nivel de desarrollo de los 6 sistemas TI a gran escala en toda la UE/Schengen, a diferencia de otros canales de información, ha sido una pieza indispensable de cooperación práctica en el ámbito de la seguridad y del control migratorio entre los Estados miembros y la UE. Es por ello, que estas fronteras inteligentes también adoptan un rol ambivalente como complejo ecosistema digital y tecnológico, llegando incluso, en ocasiones, a provocar una confusión impostada entre la finalidad de la vigilancia de las fronteras estatales por motivos de gestión migratoria y la finalidad de los controles policiales que se sirven de estas para la prevención de actos terroristas o la persecución de delitos. Aunque las fronteras inteligentes se configuren en términos resolutivos como sistemas de identificación automatizada para agilizar y facilitar el procedimiento de control fronterizo de la mayoría de los viajeros, estas no dejan de ser nuevas herramientas de contención selectiva y prospectiva con repercusiones preferentemente dirigidas sobre los flujos migratorios de nacionales de terceros países no deseados. La identificación y verificación cruzada integral de datos que está latente en el marco de interoperabilidad del ELSJ entraña el riesgo inevitable de que se produzcan efectos perjudiciales o perversos derivables de la conexión automatizada de datos entre diferentes contextos y fines. Es así incluso si la definición de los indicadores del riesgo, no se basan exclusivamente en las características personales de los individuos, sino también en circunstancias objetivas que les afectan (como los antecedentes penales o la conducta previa). El marco de la interoperabilidad, aplicado a la migración y asilo, tiende a reproducir de forma ilimitada, invisible y sesgada una serie idéntica de estereotipos sobre las personas migrantes a la hora de clasificarlos y categorizarlos.

Bajo mi punto de vista, incluso ello va a ser así, tras una lectura de las reformas legislativas derivadas del nuevo Pacto europeo o del Reglamento IA según su calendario escalonado de aplicación. En este *corpus* normativo se minimiza y se sobrestima si cabe más su futuro alcance ambivalente. No solo se obvia la plena operatividad e interoperabilidad de los sistemas de información de gran magnitud a partir del 2026 o el impacto del despliegue de los sistemas IA o los softwares algorítmicos desde y a través de las *smart borders*, sino que esta confianza y, eficiencia interesada en la *smartificación* genera riesgos y amenazas indeterminadas. Básicamente, porque el control discrecional del movimiento y la gestión discrecional de la movilidad en y hacia las fronteras inteligentes amplía las prácticas de *rebordering*, de clasificación y etiquetado automatizados reafirmando así las lógicas de inclusión/exclusión hacia la potencial persona solicitante de asilo, aquella exenta de visado o de autorización de viaje frente a la persona migrante que ha entrado de forma irregular estando bajo sospecha todas las solicitudes incluso su condición vulnerable. Entre sus riesgos, cabe destacar por no ser menor la reproducción ilimitada de categorías estereotipadas en el ámbito preventivo del triaje, o en la comprobación cruzada de identidades e información biométrica. Estas permiten distorsionar las categorizaciones jurídicas por medio de la toma de decisiones automatizadas o el cálculo aparentemente controlado de perfiles de riesgos. En definitiva, no reconoce la capacidad camaleónica de naturalización y neutralización que introducen o pueden llegar a desarrollar sistemas como el SEIAV o el VIS con independencia de su calificación o no como IA. No solo se reproducen ciertas categorías migrantes o incluso sus comportamientos por aproximación, sino que se potencian los efectos de hipervisibilidad del riesgo potencial futuro que proyectan dicha serialización estadística pues en términos algorítmicos justifican condicionar *ex ante* la posibilidad de circulación y restringir el ejercicio de derechos, especialmente agravado en el caso de los solicitantes de asilo o las movilidades en situación de mayor vulnerabilidad. Por tanto, si bien las categorizaciones del riesgo sean específicas y la estratificación jurídica de los no-nacionales europeas son necesarias para establecer estándares en la protección de derechos, las categorías estereotipadas también pueden justificar, agilizar y reforzar nuevas formas de opresión y subordinación deshumanizante hacia ellas.

Por todo ello, si bien los *critical borders studies* o los *critical data studies* han reivindicado con especial énfasis las paradojas del nexo seguridad/facilitación de las fronteras inteligentes y el conductismo de las bases de datos, por su parte, los estudiosos del derecho anti-discriminatorio ya han alertado sobre la temida resiliencia de los mecanismos jurídicos de lucha contra esta capacidad de inferencia ilimitada. Hay un desafío/preocupación compartido por explorar. No solo se trata de afrontar los efectos discriminatorios de la *smartificación* vs. *algoritmización* de la frontera en contextos migratorios globales, sino también al respecto hacer una autoevaluación crítica de sus daños. Primero, preguntarse cuál es el grado admisible de deshumanización subyacente al control migratorio y fronterizo europeo que están dispuestos a asumir y, segundo, por derivación directa cuál será la capacidad de reacción ante un punto de no retorno en el desarrollo algorítmico avanzado de tales prácticas de *re-bordering* tras el próximo 2030.

## Referencias

- Achiume, E. T., 2022. Racial Borders. *Georgetown Law Journal*, 110(3), 444-508.
- Agamben, G., 2006. *Mezzi senza fine. Note sulla politica*. Turín: Bollati e Boringhieri.

- Alonso Tomé, S., 2025. La aplicación de la inteligencia artificial en los controles de las fronteras exteriores de la Unión Europea: Regulación y desafíos. *Revista de Estudios Europeos* [en línea], 85, 588-619. Disponible en: <https://doi.org/10.24197/ree.85.2025.588-619>
- Amelung, N., y Machado, H., 2019. 'Bio-Bordering' Processes in the EU: De-Bordering and Re Bordering Along Transnational Systems of Biometric Database Technologies. *International Journal of Migration and Border Studies* [en línea], 5(4), 392-408. Disponible en: <https://doi.org/10.1504/IJMB.2019.105813>
- Amoore, L., 2006. Biometric borders: Governing mobilities in the war on terror. *Political Geography* [en línea], 25 (3), 336-351. Disponible en: <https://doi.org/10.1016/j.polgeo.2006.02.001>
- Arce Jiménez, C., 2023. Las nuevas tecnologías en las políticas migratorias y de control de fronteras españolas y europeas. un reto para la vigencia de los derechos fundamentales. *Estudios de Deusto. Revista de Derecho público* [en línea], 71(2), 15-49. Disponible en: <https://doi.org/10.18543/ed.2926>
- Avello Martínez, M., 2023. EU Borders and Potential Conflicts between New Technologies and Human Rights. *Peace & Security – Paix et Sécurité Internationales* [en línea], 11, 1-33. Disponible en: [https://doi.org/10.25267/Paix\\_secur\\_int.2023.i11.1204](https://doi.org/10.25267/Paix_secur_int.2023.i11.1204)
- Balibar, É., 2005. Fronteras del mundo, fronteras de la política. *Alteridades* [en línea], 15(30), 87-96. Disponible en: <https://www.redalyc.org/pdf/747/74703008.pdf>
- Beduschi, A., y McAuliffe, M., 2022. *Artificial Intelligence, Migration and Mobility: Implications for Policy and Practice* [en línea]. Geneva: World Migration Report (International Organization for Migration). Disponible en: <https://doi.org/10.1002/wom3.32>
- Bellanova, R., Helena Carrapico, H., y Duez, D., 2022. Digital/sovereignty and European security integration: an introduction. *European Security* [en línea], 31(3), 337-355. Disponible en: <https://doi.org/10.1080/09662839.2022.2101887>
- Bellanova, R., y Glouftsiou, G., 2022. Formatting European security integration through database interoperability. *European Security* [en línea], 31(3), 454-474. Disponible en: <https://doi.org/10.1080/09662839.2022.2101886>
- Bigo, D. 2011. Security: A Field Left Fallow', En M. Dillon, y Neal, W. *Foucault on Politics, Security and War*, Basingstoke: Palgrave Macmillan, 93-114.
- Bigo, D., 2020. Interoperability: A Political Technology for the Datafication of the Field of EU Internal Security?. En: D. Bigo et al., eds., *The Routledge Handbook of Critical European Studies* [en línea]. Londres: Routledge, 400-417. Disponible en: <https://doi.org/10.4324/9780429491306-26>
- Bigo, D., 2022. The Digitalisation of Border Controls and their Corporate Actors. En: M. Bosworth y L. Zedner, eds., *Privatising Border Control. Law at the Limits of the Sovereign State* [en línea]. Oxford University Press, 1-25. Disponible en: <https://sciencespo.hal.science/hal-03967365v1>



- Bigo, D., et al., 2012. *Evaluating Current and Forthcoming Proposals on JHA Databases and a Smart Borders System at EU External Borders*. Bruselas: Parlamento Europeo.
- Blasi Casagran, C., 2021. Fundamental rights implications of interconnecting migration and policing databases in the EU. *Human rights law review* [en línea], 21(2), 433-457. Disponible en: <https://doi.org/10.1093/hrlr/ngaa057>
- Broeders, D., 2007. The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants. *International Sociology* [en línea], 22(1), 71-92. Disponible en: <https://doi.org/10.1177/0268580907070126>
- Broeders, D., 2011. A European ‘Border’ Surveillance System under Construction. En: H. Dijstelbloem y A. Meijer, eds., *Migration and the New Technological Borders of Europe* [en línea]. Basingstoke: Palgrave MacMillan, 40–67. Disponible en: [https://doi.org/10.1057/9780230299382\\_3](https://doi.org/10.1057/9780230299382_3)
- Brunet-Jailly, E., 2006. Security and border security policies: Perimeter or smart border? A comparison of the European union and Canadian- American border security regimes. *Journal of Borderlands Studies* [en línea], 21(1), 3-21. Disponible en: <https://doi.org/10.1080/08865655.2006.9695649>
- Burgess, J.P., y Kloza, D., eds., 2021. *Border control and new technologies. Addressing integrated Impact Assessment*. Bruselas: Academic and Scientific Publishers.
- Campesi, G., 2012. Migraciones, seguridad y confines en la teoría social contemporánea. *Revista Crítica Penal y Poder*, 3, 1-20.
- Campesi, G., 2021. Geografia giuridica dei confini. *Sociologia del Diritto* [en línea], 48(3), 15-42. Disponible en: <https://doi.org/10.3280/SD2021-003002>
- Chouliaraki, L., y Georgiou, M., 2019. The digital border: Mobility beyond territorial and symbolic divides. *European Journal of Communication* [en línea], 34(6), 594-605. Disponible en: <https://doi.org/10.1177/0267323119886147>
- Comisión Europea (CE), 2008. *Commission Communication of 13 February 2008 on ‘Preparing the next steps in border management in the European Union’*. Bruselas: CE.
- Comisión Europea (CE), 2011. *Communication from the Commission to the European Parliament and the Council on Smart borders: options and the way forward*. Bruselas: EC.
- Comisión Europea (CE), 2016. *Communication from the Commission to the European Parliament and the Council on Stronger and Smarter Information Systems for Borders and Security*. Bruselas: EC.
- Comisión Europea (CE), 2020. *The Use of Artificial Intelligence in Border Control, Migration and Security*. Bruselas: EC.
- Comisión Europea (CE), 2021. *Opportunities and Challenges for the Use of Artificial Intelligence in Border Control, Migration and Security*. Bruselas: EC.
- Comisión Europea (CE), 2022. *Towards an integrated management of the external borders of the Member States of the European Union*. Bruselas: EC.

- Cook, R.J. y Cusack, S., 2010. *Gender Stereotyping: Transnational Legal Perspectives* [en línea]. Filadelfia: University of Pennsylvania Press. Disponible en: <https://doi.org/10.9783/9780812205923>
- Côté-Boucher, K., 2008. The Diffuse Border: Intelligence-Sharing, Control and Confinement along Canada's Smart Border. *Surveillance & Society* [en línea], 5(2), 142-165. Disponible en: <https://doi.org/10.24908/ss.v5i2.3432>
- Cruz Ángeles, J., 2020. Procesamiento informático de datos y protección de derechos fundamentales en las fronteras exteriores de la Unión Europea. *Freedom, Security and Justice: European legal studies* [en línea], 1, 94-122. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=7292203>
- Cruz Ángeles, J., 2022. La nueva Ley de Inteligencia Artificial una aliada necesaria para gestionar controles fronterizos, migratorios y de asilo en la Unión Europea. En: G. Vestri, ed., *La disrupción tecnológica en la Administración Pública: retos y desafíos de la inteligencia artificial*. Cizur Menor: Aranzadi, 97-121.
- Csernaton, R., 2018. Constructing the EU's high-tech borders: FRONTEX and dual-use drones for border management. *European Security* [en línea], 27(2), 175-200. Disponible en: <https://doi.org/10.1080/09662839.2018.1481396>
- De Genova, N., 2013. Spectacles of migrant 'illegality': the scene of exclusion, the obscene of inclusion. *Ethnic and Racial Studies* [en línea], 36(7), 1180-1198. Disponible en: <https://doi.org/10.1080/01419870.2013.783710>
- Derave, C., Genicot, N., y Hetmanska, N., 2022. The Risks of Trustworthy Artificial Intelligence: The Case of the European Travel Information and Authorisation System. *European Journal of Risk Regulation* [en línea], 13(3), 389-420. Disponible en: <https://doi.org/10.1017/err.2022.5>
- Dijstelbloem, H., y Broeders, D., 2015. Border surveillance, mobility management and the shaping of non-publics in Europe. *European Journal of Social Theory* [en línea], 18(1), 21-38. Disponible en: <https://doi.org/10.1177/1368431014534353>
- Dijstelbloem, H., y Meijer, A., 2011. *Migration and the new technological borders of Europe* [en línea]. Basingstoke: Palgrave Macmillan. Disponible en: <https://doi.org/10.1057/9780230299382>
- Dumbrava, C., 2021. *Artificial intelligence at EU borders. Overview of applications and key issues*. Bruselas: Servicio de Investigación del Parlamento Europeo.
- Epstein, E., 2007. Guilty Bodies, Productive Bodies, Destructive Bodies: Crossing the Biometric Borders. *International Political Sociology* [en línea], 1(2), 149-164. Disponible en: <https://doi.org/10.1111/j.1749-5687.2007.00010.x>
- European Digital Rights (EDRi), 2022. *Uses of AI in immigration and border control. A fundamental rights approval to the Artificial Intelligence Act* [en línea]. Bruselas: EDRi. Disponible en: [https://edri.org/wp-content/uploads/2022/05/Migration\\_2-pager-02052022-for-online.pdf](https://edri.org/wp-content/uploads/2022/05/Migration_2-pager-02052022-for-online.pdf)
- European Migration Network (EMN), 2022. *The use of digitalization and artificial intelligence in migration management*. Informe. Febrero. Bruselas: EMN.

- Everuss, L., 2021. AI, smart borders and migration. En: A. Elliott, ed., *The Routledge Social Science Handbook of AI* [en línea]. Londres: Routledge, 339-356. Disponible en: <https://doi.org/10.4324/9780429198533-23>
- Forti, M., 2024. Addressing Algorithmic Errors in Data-Driven Border Control Procedures. *German Law Journal* [en línea], 25(1), 1-11. Disponible en: <https://doi.org/10.1017/glj.2023.102>
- Foucault, M. (con A.I. Davidson, ed.), 2008. *Birth of Biopolitics: Lectures at the Collège de France, 1978-1979*. Nueva York: Palgrave Macmillan.
- Gäckle, N., 2020. Taming future mobilities: biopolitics and data behaviourism in the European Travel Information and Authorisation System (ETIAS). *Mobilities* [en línea], 15(2), 257-272. Disponible en: <https://doi.org/10.1080/17450101.2019.1693725>
- Garrido Carrillo, F.J., 2023. La inteligencia artificial en el control de los flujos migratorios en la Unión Europea. La necesidad de un marco normativo garantista de los derechos fundamentales. *Revista General de Derecho Europeo*, 60, 1-39.
- Ghidoni, E., y Morondo, D., 2023. El papel de los estereotipos en las formas de desigualdad compleja: algunos apuntes desde la teoría feminista del derecho antidiscriminatorio. *Discusiones* [en línea], 28, 37-70. Disponible en: <https://doi.org/10.52292/j.dsc.2022.2325>
- Goldner Lang, I., 2024. Security-centric approach in the use of digital technologies in EU migration and asylum policies. *Transnational Legal Theory* [en línea], 15(4), 591-599. Disponible en: <https://doi.org/10.1080/20414005.2024.2399934>
- Guild, E., Mitsilegas, V., y Vavoula, N., 2025. *Lawless Borders. The Rule of Law Deficit in European Immigration Control* [en línea]. Bristol University Press. Disponible en: <https://doi.org/10.56687/9781529237801>
- Harcourt, B.E., 2007. *Against prediction. Profiling, policing, and punishing in an actuarial age* [en línea]. The University of Chicago Press. Disponible en: <https://doi.org/10.7208/chicago/9780226315997.001.0001>
- Hayes, V., y Vermeulen, M., 2012. *Borderline, the EU's New Border Surveillance Initiatives*. Berlín: Heinrich Böll Foundation.
- Jasmontaite-Zaniewicz, L., y Zomignani Barboza, J., 2021. Disproportionate surveillance: technology assisted and automated decisions in asylum applications in the EU?. *International Journal of Refugee Law* [en línea], 33, 89-110. Disponible en: <https://doi.org/10.1093/ijrl/eeab031>
- Jeandesboz, J., 2016. Smartening border security in the European Union: An associational inquiry. *Security Dialogue* [en línea], 47(4), 292-309. Disponible en: <https://doi.org/10.1177/0967010616650226>
- Jeandesboz, J., et al., 2013. *The Commission's Legislative Proposals on Smart Borders: Their Feasibility and Costs*. Bruselas: Directorate General for Internal Policies. Policy Department C: Citizen's Rights and Constitutional Affairs.

- Josipovic, I., 2024. Digitalising Asylum Procedures: The Legitimation of Smartphone Data Extraction for Retrospective Border Control. *Geopolitics* [en línea], 29(5), 1831-1854. Disponible en: <https://doi.org/10.1080/14650045.2023.2288162>
- Kilpatrick, J., y Jones, C., 2022. *A clear and present danger. Missing safeguards on immigration and asylum EU's AI act*. Londres: Statewatch.
- Korkmaz, E.E., 2024. *Smart borders, digital identity and big data: how surveillance technologies are used against migrants* [en línea]. Bristol University Press. Disponible en: <https://doi.org/10.1332/policypress/9781529233506.001.0001>
- La Spina, E., 2024. La regulación europea de la IA ante los sesgos y riesgos de discriminación algorítmica en contextos migratorios. *Revista CIDOB d'Afers Internacionals* [en línea], 138, 171-194. Disponible en: <https://doi.org/10.24241/rcai.2024.138.3.171>
- Leese, M., 2014. The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue* [en línea], 45(5), 494-511. Disponible en: <https://doi.org/10.1177/0967010614544204>
- Leese, M., 2016. Exploring the Security/Facilitation Nexus: Foucault at the 'Smart' Border. *Global Society* [en línea], 30(3), 412-429. Disponible en: <https://doi.org/10.1080/13600826.2016.1173016>
- Leese, M., Noori, S., y Scheel, S., 2022. Data Matters: The Politics and Practices of Digital Border and Migration Management. *Geopolitics* [en línea], 27(1), 5-25. Disponible en: <https://doi.org/10.1080/14650045.2021.1940538>
- Lehtonen, P., y Aalto, P., 2017. Smart and secure borders through automated border control systems in the EU? The views of political stakeholders in the Member States. *European Security* [en línea], 26(2), 207-225. Disponible en: <https://doi.org/10.1080/09662839.2016.1276057>
- Lyon, D., 2005. The border is everywhere: ID cards, surveillance and the other. En: E. Zuriek y M. Salter, eds., *Global Surveillance and Policing. Borders, security, identity*. Londres: Willan, 66-82.
- Marin, L., 2011. Is Europe Turning into a 'Technological Fortress'? Innovation and Technology for the Management of EU's External Borders. En: M. Heldeweg y E. Kica, eds., *Regulating Technological Innovation: Legal and Economic Regulation of Technological Innovation* [en línea]. Londres: Palgrave Macmillan, 131-151. Disponible en: [https://doi.org/10.1057/9780230367456\\_8](https://doi.org/10.1057/9780230367456_8)
- Méndez-Fierros, H., 2023. La frontera digital Estados Unidos-México. Representaciones de tecnología y construcción mediática del migrante irregular como amenaza-enemigo. *Estudios Fronterizos* [en línea], 24, 1-28. Disponible en: <https://doi.org/10.21670/ref.2317128>
- Michéa, F., y Rousvoal, L., 2021. The Criminal Procedure Out of Itself: A Case Study of The Relationship Between EU Law and Criminal Procedure Using the ETIAS System. *European Papers*, 6(1), 473-491.

- Molnar, P., 2019. Technology on the Margins: AI and Global Migration Management from a Human Rights Perspective. *Cambridge International Law Journal* [en línea], 8(2), 305-330. Disponible en: <https://doi.org/10.4337/cilj.2019.02.07>
- Molnar, P., 2023. Digital border technologies, techno-racism and logics of exclusion. *International Migration* [en línea], 61(5), 307-312. Disponible en: <https://doi.org/10.1111/imig.13187>
- Molnar, P., 2024. *AI surveillance and border tech experiments*. Nueva York: The New Press.
- Muller, B.J., 2009. Borders, Risks, Exclusions. *Studies in Social Justice* [en línea], 3(1), 67–78. Disponible en: <https://doi.org/10.26522/ssj.v3i1.1024>
- Musco Eklund, A., 2023. Rule of Law Challenges of ‘Algorithmic Discretion’ & Automation in EU Border Control. A Case Study of ETIAS Through the Lens of Legality. *European Journal of migration and Law* [en línea], 25(3), 249-274. Disponible en: <https://doi.org/10.1163/15718166-12340152>
- Nedelcu, M., y Soysüren, I., 2020. Precarious migrants, migration regimes and digital technologies: the empowerment-control nexus. *Journal of Ethnic and Migration Studies* [en línea], 48(8), 1821-1837. Disponible en: <https://doi.org/10.1080/1369183X.2020.1796263>
- Nobile, R., 2024. La vulnerabilità del migrante nell’era delle *smart-borders* e delle tecnologie *lie-detecting*. *BioLaw Journal – Rivista di BioDiritto*, 1, 289-301.
- Oliveira Martins, B., y Gabrielsen Jumbert, M., 2022. EU Border technologies and the co-production of security ‘problems’ and ‘solutions’. *Journal of Ethnic and Migration Studies* [en línea], 48(6), 1430-1447. Disponible en: <https://doi.org/10.1080/1369183X.2020.1851470>
- Ozkul, D., 2023. *Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe*. Refugee Studies Centre, University of Oxford.
- Penasa, S., 2022. Artificial intelligence and the governance of migration: potentialities and pitfalls between technological neutrality and political design. *Opinio juris in comparatione*, 1, special issue, 94-113.
- Pöttsch, H., 2015. The emergence of iBorder: Bordering bodies, networks, and machines. *Environment and Planning D: Society and Space* [en línea], 33(1), 101–118. Disponible en: <https://doi.org/10.1068/d14050p>
- Pöttsch, H., 2018. iBorder/ing. En: C. Lury y E. Uprichard, eds., *Routledge Handbook of Interdisciplinary Research Methods* [en línea]. Londres: Routledge. 99–103. Disponible en: <https://doi.org/10.4324/9781315714523-13>
- Romano, A., 2023. Derechos fundamentales e inteligencia artificial emocional en iBorderCtrl: retos de la automatización en el ámbito migratorio. *Revista Catalana de Dret Públic* [en línea], 66, 237-252. Disponible en: <https://doi.org/10.58992/rcdp.i66.2023.3928>



- San Martín Segura, D., 2019. Las lógicas de gobierno de lo fronterizo en el espacio Schengen: la frontera como estriación. *Revista CIDOB d'Afers Internacionals* [en línea], 122, 15-37. Disponible en: <https://doi.org/10.24241/rcai.2019.122.2.15>
- San Martín Segura, D., 2025. The quantification of behavioural forecast in administrative legal practice: the algorithmic risk assessment of the ETIAS, *Federalismi.it*, 3, 564-606.
- Sassen, S., 2006. *Territory, authority, rights: from medieval to Global assemblages*. Princeton University Press.
- Scheel, S., 2024. Epistemic domination by data extraction: questioning the use of biometrics and mobile phone data analysis in asylum procedures. *Journal of Ethnic and Migration Studies* [en línea], 50(9), 2289-2308. Disponible en: <https://doi.org/10.1080/1369183X.2024.2307782>
- Sontowski, S., 2018. Speed, timing and duration: contested temporalities, techno-political controversies and the emergence of the EU's smart border. *Journal of Ethnic and Migration Studies* [en línea], 44(6), 2730-2746. Disponible en: <https://doi.org/10.1080/1369183X.2017.1401512>
- Tassinari, F., 2022. *The external reach of the interoperability of large-scale IT systems in the AFSJ*. Tesis Doctoral. Universidad de Granada.
- Tassinari, F., 2025. La interoperabilidad en el espacio de libertad, seguridad, y justicia y el nuevo Reglamento de Inteligencia Artificial. Algunas consideraciones sobre el procedimiento de detección de identidades múltiples. *InDret* [en línea], 2, 346-386. Disponible en: <https://doi.org/10.31009/InDret.2025.i2.08>
- Taylor, L., y Meissner, F., 2020. A Crisis of Opportunity: Market-Making, Big Data, and the Consolidation of Migration as Risk. *Antipode* [en línea], 52(1), 270-290. Disponible en: <https://doi.org/10.1111/anti.12583>
- Topak, O.E., et al., 2015. From Smart Borders to Perimeter Security: The Expansion of Digital Surveillance at the Canadian Borders. *Geopolitics* [en línea], 20(4), 880-89. Disponible en: <https://doi.org/10.1080/14650045.2015.1085024>
- Trauttmansdorff, P., 2017. The Politics of Digital Borders. En: C. Günay y N. Witjes, eds., *Border Politics: Defining Spaces of Governance and Forms of Transgressions* [en línea]. Cham: Springer, 107-126. Disponible en: [https://doi.org/10.1007/978-3-319-46855-6\\_7](https://doi.org/10.1007/978-3-319-46855-6_7)
- Van Dijck, T., 2014. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & society* [en línea], 12(2), 197-208. Disponible en: <https://doi.org/10.24908/ss.v12i2.4776>
- Vantin, S., 2021. *Il diritto antidiscriminatorio nell'era digitale. Potenzialità e rischi per le persone, La Pubblica Amministrazione, le imprese*. Milán: Wolters Kluwer.
- Vaughan-Williams, N., 2009. The generalised bio-political border? Re-conceptualising the limits of sovereign power. *Review of International Studies* [en línea], 35(4), 729-749. Disponible en: <https://doi.org/10.1017/S0260210509990155>

- Vavoula, N., 2021. Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism. *European Journal of Migration and Law* [en línea], 23, 457-484. Disponible en: <https://doi.org/10.1163/15718166-12340114>
- Velasco Rico, C.I., y Laukyte, M., 2024. ETIAS system and new proposals to advance the use of AI in public services. *Law & Security Review* [en línea], 54, 1-9. Disponible en: <https://doi.org/10.1016/j.clsr.2024.106015>
- Velasco, J.C., 2022. Prolegómenos a una filosofía política de la frontera. Historia, concepto y mutaciones contemporáneas. *Daimon. Revista Internacional de Filosofía* [en línea], 87, 11-27. Disponible en: <https://doi.org/10.6018/daimon.526121>
- Velasco, J.C., 2025. *Anatomía de la frontera*. Madrid: Tecnos.
- Vrăbiescu, J., 2022. Deportation, smart borders and mobile citizens: using digital methods and traditional police activities to deport EU citizens. *Journal of Ethnic and Migration Studies* [en línea], 48(8), 1891-1908. Disponible en: <https://doi.org/10.1080/1369183X.2020.1796267>
- Walters, W., 2006. Border/Control. *European Journal of Social Theory* [en línea], 9(2), 187-203. Disponible en: <https://doi.org/10.1177/1368431006063332>